PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-011101

(43)Date of publication of application : 14.01.2000

(51)Int.Cl. G06K 17/00
G06F 3/06
G06F 3/08
G06K 19/073
G06K 19/07

(21)Application number : 10-173163

(22)Date of filing : 19.06.1998

(71)Applicant : HITACHI LTD

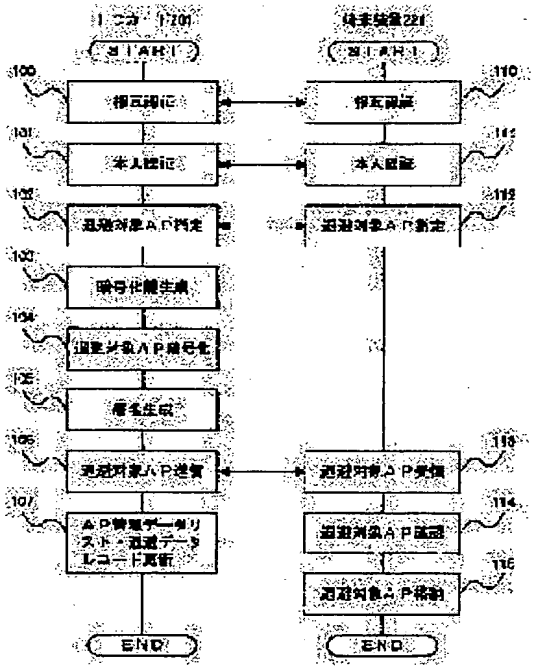
(72)Inventor : FUKUZAWA YASUKO
ORIMO MASAYUKI
HARAGUCHI MASATOSHI

(54) IC CARD AND RECORD MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To save an application program(AP) stored in an IC card according to the judgment of a user, and to prevent the illegal use of the saved AP.

SOLUTION: An IC card 201 generates and manages an arbitrary cryptographic key, and enciphers an AP to be saved among APS stored in an internal memory by using this cryptographic key, and saves this AP through an IC card reader/writer 211 to a connected terminal equipment 221, and deletes the AP before encipherment. Also, at the time of restoring the saved AP, the IC card 201 decodes the AP received from the terminal equipment 221 by using the managed cryptographic key, and restores the AP in the internal memory.



LEGAL STATUS

[Date of request for examination] 15.08.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－11101
（P2000－11101A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｂ	５Ｂ０３５
			Ｅ	５Ｂ０５８
Ｇ０６Ｆ　3/06	３０４	Ｇ０６Ｆ　3/06	３０４Ｈ	５Ｂ０６５
3/08		3/08	Ｃ	
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平10－173163

(22)出願日　平成10年６月19日(1998.6.19)

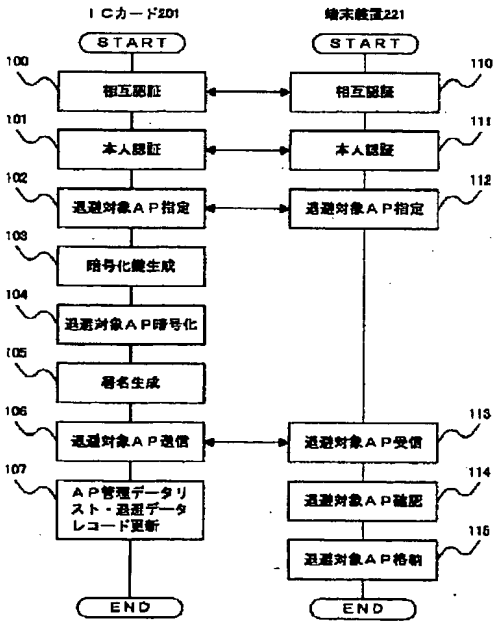
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　福澤　寧子
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　織茂　昌之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100087170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　ＩＣカードおよび記録媒体

(57)【要約】
【課題】ＩＣカードに格納されているアプリケーションプログラム（ＡＰ）を、ユーザの判断で退避させることを可能とすると共に、退避させてあるＡＰの不正使用を防止する。
【解決手段】ＩＣカード２０１は、任意の暗号化鍵を生成して管理し、内部のメモリ２０２に格納されているＡＰのうちの、退避対象とするＡＰを、この暗号化鍵を用いて暗号化してから、ＩＣカードリーダ／ライタ２１１を介して接続される端末装置２２１に退避させ、暗号化前のＡＰを消去する。また、ＩＣカード２０１は、退避させておいたＡＰを回復させる際には、端末装置２２１から受け取ったＡＰを、管理しておいた暗号化鍵を用いて復号し、内部のメモリ２０２に再格納する。

図１



1

【特許請求の範囲】
【請求項１】１つ以上のデータが内部のメモリに格納されているＩＣカードであって、
退避対象とするデータの指定を外部から受け付ける手段と、
任意の暗号化鍵を生成する手段と、
退避対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを消去する手段と、
生成した暗号化鍵を記憶する手段と、
暗号化後のデータを外部に退避させる手段と、
退避させておいたデータを外部から受け取る手段と、
受け取ったデータを、記憶しておいた暗号化鍵を用いて復号する手段と、
復号後のデータを内部のメモリに再格納する手段とを備えたことを特徴とするＩＣカード。
【請求項２】１つ以上のデータが内部のメモリに格納されているＩＣカードであって、
無効化対象とするデータの指定を外部から受け付ける手段と、
任意の暗号化鍵を生成する手段と、
無効化対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを暗号化後のデータに置き換える手段と、
生成した暗号化鍵を記憶する手段と、
有効化対象とするデータの指定を外部から受け付ける手段と、
有効化対象として受け付けたデータを、記憶しておいた暗号化鍵を用いて復号する手段とを備えたことを特徴とするＩＣカード。
【請求項３】請求項１または２記載のＩＣカードであって、
内部のメモリに格納されている１つ以上のデータは、アプリケーションプログラムを含むことを特徴とするＩＣカード。
【請求項４】請求項１記載のＩＣカードがＩＣカードリーダ／ライタを介して接続される端末装置にインストールされるプログラムを記録した記録媒体であって、
上記ＩＣカードに格納されている１つ以上のデータのうちの、退避対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ＩＣカードに出力する手段と、
上記ＩＣカードから退避させられたデータを受け取って、上記端末装置のメモリに格納する手段と、
上記ＩＣカードから退避させられて上記端末装置に格納されているデータのうちの、回復対象となるデータの指定を受け付ける手段と、
回復対象として受け付けたデータを上記ＩＣカードに出力する手段とを、上記端末装置が備えるよう動作させるプログラムを記録したことを特徴とする記録媒体。

2

【請求項５】請求項２記載のＩＣカードがＩＣカードリーダ／ライタを介して接続される端末装置にインストールされるプログラムを記録した記録媒体であって、
上記ＩＣカードに格納されている１つ以上のデータのうちの、無効化対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ＩＣカードに出力する手段と、
上記ＩＣカードに格納されているデータのうちの、有効化対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ＩＣカードに出力する手段とを、上記端末装置が備えるよう動作させるプログラムを記録したことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、１つ以上のデータが格納されているＩＣカードを運用管理する技術に係り、特に、セキュリティニーズに対する解決策を提示する技術に関するものである。
【０００２】
【従来の技術】従来は、アプリケーションプログラム（以下、「ＡＰ」と称す。）が利用するデータのみをＩＣカードに格納しておき、ＩＣカードリーダ／ライタを介してこのデータを読み取った端末装置側で、ＡＰを動作させるようにした利用形態が一般的であった。
【０００３】これに対し、近年、ＩＣカード上でＡＰを動作させるための基本ソフト（カードＯＳ）をＩＣカードに格納することで、ＡＰをＩＣカードに格納する動きが大きくなりつつある。
【０００４】また、複数のＡＰを１枚のＩＣカードに格納し、複数のＩＣカードを１枚のＩＣカードに統合することで、操作性を向上させ、ＩＣカードのコストを、ＡＰ発行機関でシェアすることが期待されている。
【０００５】なお、カードＯＳの一例としては、ＭＵＬＴＯＳが知られている。
【０００６】ＭＵＬＴＯＳは、Fuji-Keizai ＵＳＡ「日米欧における電子アドバンス・カードのトレンドと今後のディレクション」という文献に記述がなされているように、ＩＣカードに出力された様々なＡＰが、ＩＣカードへのロードを正しく許可されたものか否かをチェックすると共に、個々のＡＰが、特殊なファイアウォール・プログラムによって分割して記録され、他のＡＰが動作を妨害しないことを保証している。ＩＣカードへのロードが正しく許可されたものか否かをチェックするために、ＡＰのロードに先立って、管理機関は、ＡＰの正当性を検証し、正規利用者のＩＣカードにのみロードされることを保証する処理を行う。ＩＣカードにロードされたＡＰのデリートも、ロードと同様にチェックしてから行われるため、管理機関によって、該等するＩＣカードからのデリートの正当性を保証する必要がある。
【０００７】

【発明が解決しようとする課題】ＭＵＬＴＯＳは、管理機関の許可のないＡＰをＩＣカードにロードすることができず、ＡＰがＩＣカードに無制限にコピーされることを防ぐことができるので、有効な管理を実現することができることから、カードＯＳとして普及していきつつある。

【０００８】しかしながら、このような厳密な管理は、ＩＣカードの利用状況に応じて、ユーザの判断で、複数のＡＰが格納されたＩＣカードから、特定のＡＰだけを一時的に退避させるような、フレキシブルな運用を制限してしまう。

【０００９】例えば、第三者が一時的にＩＣカードを利用するときや、メモリ量の制約などから、しばらく必要としないＡＰをＩＣカードから退避させ、使用したい他のＡＰと置き換えたい場合には、ユーザの判断で、ＩＣカードに格納されているＡＰを退避させて無効化し、また、退避させておいたＡＰを回復させることが望まれる。

【００１０】しかし、ＭＵＬＴＯＳをカードＯＳとしているＩＣカードにおいては、上述したように、ＩＣカードからのＡＰのデリート時にも管理機関の許可を必要とするので、ユーザの判断で、一時的にＡＰを退避させるような運用はできない。

【００１１】本発明の目的は、ＩＣカードに格納されているデータを、ユーザの判断で退避させることを可能とすると共に、退避させてあるデータの不正使用を防止することを可能とすることにある。

【００１２】

【課題を解決するための手段】上記目的を達成するために、本発明は、ＩＣカードに格納されているデータを、ＩＣカード内で生成した暗号化鍵を用いてＩＣカード内で暗号化し、暗号化後のデータをＩＣカードから退避させるようにしている。また、生成した暗号化鍵をＩＣカード内で管理しておき、退避させておいたデータを回復させる際には、このデータを、ＩＣカード内で管理しておいた暗号化鍵を用いてＩＣカード内で復号するようにしている。

【００１３】すなわち、本発明は、第１の態様として、１つ以上のデータが内部のメモリに格納されているＩＣカードであって、退避対象とするデータの指定を外部から受け付ける手段と、任意の暗号化鍵を生成する手段と、退避対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを消去する手段と、生成した暗号化鍵を記憶する手段と、暗号化後のデータを外部に退避させる手段と、退避させておいたデータを外部から受け取る手段と、受け取ったデータを、記憶しておいた暗号化鍵を用いて復号する手段と、復号後のデータを内部のメモリに再格納する手段とを備えたことを特徴としたＩＣカードを提供している。

【００１４】第１の態様によれば、ＩＣカードから退避させられたデータは、これを暗号化したＩＣカード以外では復号できないので、不正使用されることがなくなる。

【００１５】ここで、暗号化したデータをＩＣカードから退避させる必要がない場合には、暗号化前のデータを暗号化後のデータに置き換えるようにすればよい。

【００１６】すなわち、本発明は、第２の態様として、１つ以上のデータが内部のメモリに格納されているＩＣカードであって、無効化対象とするデータの指定を外部から受け付ける手段と、任意の暗号化鍵を生成する手段と、無効化対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを暗号化後のデータに置き換える手段と、生成した暗号化鍵を記憶する手段と、有効化対象とするデータの指定を外部から受け付ける手段と、有効化対象として受け付けたデータを、記憶しておいた暗号化鍵を用いて復号する手段とを備えたことを特徴としたＩＣカードを提供している。

【００１７】なお、第１の態様および第２の態様のＩＣカードいずれにおいても、内部のメモリに格納されている１つ以上のデータは、ＡＰを含むようにすることができるのは、当然である。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００１９】図２は、本実施形態に係るＩＣカードシステムの全体構成図である。

【００２０】図２に示すように、本実施形態に係るＩＣカードシステムは、ユーザが所有するＩＣカード２０１と、端末装置２２１とが、ＩＣカードリーダ／ライタ２１１を介して接続された構成となっている。

【００２１】ＩＣカード２０１は、ＭＰＵ２０３と、メモリ２０２と、送受信ＩＦ２０４とを備えて構成され、端末装置２２１は、ＭＰＵ２２３と、メモリ２２２と、キーボード２２４と、ディスプレイ２２５と、送受信ＩＦ２２６とを備えて構成されている。

【００２２】また、ＩＣカードリーダ／ライタ２１１は、送受信ＩＦ２１２と、送受信ＩＦ２１３とを備えて構成されている。

【００２３】ＩＣカード２０１および端末装置２２１は、ＩＣカードリーダ／ライタ２１１を介して送受信を行うが、通信の形態は有線／無線を問わない。

【００２４】次に、ＩＣカード２０１のメモリ２０２に格納されている内容について、図３を用いて説明する。

【００２５】図３に示すように、ＩＣカード２０１のメモリ２０２には、例えば、クレジットやＧＳＭ（global system for mobile communication）等の、１つ以上ＡＰが格納されているが、ここでは、ＡＰ＃１（３２１）およびＡＰ＃２（３２２）が格納されているものとする。

【００２６】また、図３に示すように、ＩＣカード２０１のメモリ２０２には、ＩＣカード２０１ごとに固有の識別子であるカード識別子３１１と、非対称暗号における認証局の公開鍵３１２と、非対称暗号におけるＩＣカード２０１の秘密鍵３１３と、非対称暗号におけるＩＣカード２０１の公開鍵３１４と、ＡＰ管理情報３１５と、ＩＣカード２０１へのアクセスを許可するためのパスワード３１６とが格納されている。

【００２７】図７はＡＰ管理情報３１５の一例を示す図である。

【００２８】ＡＰ管理情報３１５は、ＩＣカード２０１のメモリ２０２に格納されているＡＰ（ここでは、ＡＰ＃１（３２１）およびＡＰ＃２（３２２）である。）の各々に対応するＡＰ管理データリスト７００から構成されている。

【００２９】図７に示すように、ＡＰ＃１（３２１）のＡＰ管理データリスト７００は、ＡＰ＃１（３２１）の識別子であるＡＰ識別子７０１と、ＡＰファイル情報７０２と、ＡＰ＃１（３２１）をＩＣカード２０１へロードした回数を示すロードカウンタ７０３と、ＡＰ＃１（３２１）をＩＣカード２０１からデリートした回数を示すデリートカウンタ７０４と、図８に示す退避データレコード８００へのポインタ７０５と、次のＡＰであるＡＰ＃２（３２２）のＡＰ管理データリスト７００へのエントリポインタ７０６とから構成されている。

【００３０】なお、ＡＰ＃２（３２２）のＡＰ管理データリスト７００も同様の構成である。

【００３１】また、ポインタ７０５には、対応するＡＰを退避させていないならば、「ＮＵＬＬ」が設定され、対応するＡＰを退避させているならば、退避データレコード８００へのポインタが、ＡＰの退避が完了した時点で設定される。なお、退避データレコード８００の詳細については後述する。

【００３２】図３に戻って、ＩＣカード２０１のメモリ２０２には、ＡＰ退避プログラム３０３と、ＡＰ回復プログラム３０４と、暗号化鍵生成プログラム３０５と、署名生成プログラム３０６と、対称暗号系暗号化／復号プログラム３０７と、非対称暗号系暗号化／復号プログラム３０８とが格納されている。

【００３３】次に、端末装置２２１のメモリ２２２に格納されている内容について、図４を用いて説明する。

【００３４】図４に示すように、端末装置２２１のメモリ２２２には、端末装置２２１ごとに固有の識別子である端末識別子４１１と、非対称暗号における認証局の公開鍵４１２とが格納されている。

【００３５】また、図４に示すように、端末装置２２１のメモリ２２２には、ＡＰ退避プログラム４０３と、ＡＰ回復プログラム４０４と、署名検証プログラム４０５と、対称暗号系暗号化／復号プログラム４０６と、非対称暗号系暗号化／復号プログラム４０７とが格納されている。

【００３６】なお、ＩＣカード２０１のメモリ２０２および端末装置２１１のメモリ２２２に格納される各種データは、各々、生成／発行／管理機関を設けることが考えられるが、ここでは、一般的に存在する認証局によって認証された公開鍵（認証局によって署名が施された公開鍵）を含む各種データが既に設定されているものとする。

【００３７】次に、本実施形態に係るＩＣカードシステムにおいて、ＩＣカード２０１に格納されているＡＰを端末装置２２１に退避させる際の動作について、図１を用いて説明する。

【００３８】図１は、本実施形態に係るＩＣカードシステムにおけるＡＰ退避時の動作の流れを示す図である。

【００３９】端末装置２２１でＡＰ退避プログラム４０３が起動され、ＩＣカード２０１がＩＣカードリーダ／ライタ２１１に挿入されると、ＩＣカード２０１でＡＰ退避プログラム３０３が起動され、以下の処理が実行される。なお、以下の処理は、ＩＣカード２０１のＭＰＵ２０３および端末装置２２１のＭＰＵ２２３が、ＡＰ退避プログラム３０３およびＡＰ退避プログラム４０３を実行することで実現される。

【００４０】まず、ＩＣカード２０１および端末装置２１１は、相互認証を行う（ステップ１００，ステップ１１０）。相互認証については、例えば、ＩＳＯ（ＩＳＯ９７９８－３）に、非対称鍵暗号を用いた認証方式が規定されており、また、ＩＳＯ（ＩＳＯ９７９８－２）に、対称鍵暗号を用いた認証方式が規定されているので、ここでは詳細を省略する。

【００４１】続いて、ＩＣカード２０１および端末装置２１１は、本人認証を行う（ステップ１０１，ステップ１１１）。

【００４２】本人認証においては、詳しくは、まず、端末装置２２１が、ディスプレイ２２５を介して、パスワードの入力をユーザに要求し、ユーザがキーボード２２４から入力したパスワードを、ＩＣカード２０１に送信する（ステップ１１１）。

【００４３】そして、ＩＣカード２０１が、端末装置２１１からパスワードを受信すると、受信したパスワードとメモリ２０２に格納されているパスワード３１６とを比較し、正しいユーザであるか否かを認証する（ステップ１０１）。なお、ＩＣカード２０１による認証結果は、端末装置２１１に通知される。

【００４４】さて、正しいユーザであることが認証された場合は、ＩＣカード２０１および端末装置２１１は、退避対象ＡＰの指定を行う（ステップ１０２，ステップ１１２）。

【００４５】退避対象ＡＰの指定においては、詳しくは、まず、端末装置２２１が、ＩＣカード２０１に格納されているＡＰの一覧を、ＩＣカード２０１から取得し

てディスプレイ２２５に表示し、ユーザがキーボード２２４から指定したＡＰを、退避対象ＡＰとして、ＩＣカード２０１に通知する（ステップ１１２）。なお、退避対象ＡＰの通知は、図５に示すＡＰ指定データレコード５００を送信することで行われる。

【００４６】図５はＡＰ指定データレコード５００の一例を示す図である。

【００４７】図５に示すように、ＡＰ指定データレコード５００は、退避対象ＡＰを一意に指定するための識別子であるＡＰ識別子５０１と、端末装置２２１の端末識別子（メモリ２２２に格納されている端末識別子４１１）５０２と、退避対象ＡＰの指定を端末装置２２１が受け付けた日時を示すタイムスタンプ５０３とから構成されている。

【００４８】そして、ＩＣカード２０１が、端末装置２１１からＡＰ指定データレコード５００を受信することで、退避対象ＡＰの指定を受け付ける（ステップ１０２）。

【００４９】続いて、ＩＣカード２０１は、ＡＰ指定データレコード５００を受信すると、暗号化鍵生成プログラム３０５を起動することによって、退避対象ＡＰを暗号化するための暗号化鍵を生成する（ステップ１０３）。ここでは、退避対象ＡＰを対称暗号で暗号化するものとし、生成する暗号化鍵は、対称暗号における暗号化鍵（例えば、乱数）である。

【００５０】続いて、ＩＣカード２０１は、対称暗号系暗号化／復号プログラム３０８を起動することによって、ステップ１０３で生成した暗号化鍵を用いて、退避対象ＡＰを暗号化すると共に、暗号化前のＡＰを消去する（ステップ１０４）。

【００５１】続いて、ＩＣカード２０１は、署名生成プログラム３０６を起動することによって、署名を生成する（ステップ１０５）。

【００５２】ステップ１０５では、詳しくは、ＩＣカード２０１は、図９に示す署名生成用データレコード９００から、ハッシュ関数を用いて認証子を生成し、非対称暗号系暗号化／復号プログラム３０８を起動することによって、メモリ２０２に格納されているＩＣカード２００の秘密鍵３１３を用いて、生成した認証子を暗号化して、署名を生成する。なお、ハッシュ関数および署名生成の詳細は、例えば、岡本龍明他著「現代暗号」，産経図書発行を参照されたい。

【００５３】図９は署名生成用データレコード９００の一例を示す図である。

【００５４】図９に示すように、署名生成用データレコード９００は、退避対象ＡＰのＡＰ識別子９０１と、暗号化した退避対象ＡＰ９０２と、端末識別子（端末装置２２１から受信したＡＰ指定データレコード５００中の端末識別子５０２）９０３と、タイムスタンプ（端末装置２２１から受信したＡＰ指定データレコード５００中のタイムスタンプ５０３）９０４と、ＩＣカード２０１のカード識別子（メモリ２０２に格納されているカード識別子３１３）９０５とから構成されている。

【００５５】続いて、ＩＣカード２０１および端末装置２１１は、暗号化した退避対象ＡＰの送受信を行う（ステップ１０６，ステップ１１３）。

【００５６】暗号化した退避対象ＡＰの送受信においては、詳しくは、まず、ＩＣカード２０１が、暗号化した退避対象ＡＰを、端末装置２２１に送信する（ステップ１０６）。なお、暗号化した退避対象ＡＰの送信は、図６に示す退避ＡＰデータレコード６００を送信することで行われる。

【００５７】図６は退避ＡＰデータレコード６００の一例を示す図である。

【００５８】図６に示すように、退避ＡＰデータレコード６００は、暗号化した退避対象ＡＰのＡＰ識別子６０１と、ステップ１０４で暗号化した退避対象ＡＰ６０２と、ＩＣカード２０１のカード識別子（メモリ２０２に格納されているカード識別子３１３）６０３と、ステップ１０５で生成した署名６０４と、ＩＣカード２０１の公開鍵６０５（メモリ２０２に格納されている公開鍵３１４）とから構成されている。

【００５９】そして、端末装置２２１が、ＩＣカード２０１から退避ＡＰデータレコード６００を受信することで、暗号化された退避対象ＡＰを受信する（ステップ１１３）。

【００６０】さて、端末装置２２１は、退避ＡＰデータレコード６００を受信すると、署名検証プログラム４０５を起動することによって、退避ＡＰデータレコード６００中の署名６０４を検証する（ステップ１１４）。

【００６１】ステップ１１４では、詳しくは、端末装置２２１は、非対称暗号系暗号化／復号プログラム４０７を起動することによって、まず、退避ＡＰデータレコード６００中の公開鍵６０５を、認証局の公開鍵４１２を用いて復号して、公開鍵６０５を検証し、続いて、退避ＡＰデータレコード６００中の署名６０４を、検証した公開鍵６０５を用いて復号して、署名６０４を検証する。

【００６２】そして、端末装置２２１は、ステップ１１４による検証の結果、退避ＡＰデータレコード６００がＩＣカード２０１から送信されたものであること、および、退避ＡＰデータレコード６００が改ざんされていないことを確認すると、退避ＡＰデータレコード６００を、メモリ２２２またはディスク装置等に格納する（ステップ１１５）。なお、端末装置２２１は、ＡＰの退避に成功した旨をＩＣカード２０１に通知する。

【００６３】そこで、ＩＣカード２０１は、ＡＰの退避に成功した旨が端末装置２２１から通知されると、対応するＡＰ管理データリスト７００を更新する（ステップ１０７）。

【００６４】ステップ１０７では、具体的には、ＩＣカード２０１は、退避データレコード８００を生成し、生成した退避データレコード８００へのポインタを、対応するＡＰ管理データリスト７００中のポインタ７０５に設定する。

【００６５】図８は退避データレコード８００の一例を示す図である。

【００６６】図８に示すように、退避データレコード８００は、端末識別子（端末装置２２１から受信したＡＰ指定データレコード５００中の端末識別子５０２）８０１と、タイムスタンプ（端末装置２２１から受信したＡＰ指定データレコード５００中のタイムスタンプ５０３）８０２と、ステップ１０３で生成した暗号化鍵８０３と、ステップ１０５で生成した署名８０４とから構成されている。

【００６７】以上に説明した動作によって、ＩＣカード２０１に格納されているＡＰを、端末装置２２１に退避させることができる。

【００６８】なお、図１に示した動作においては、対称暗号で退避対象ＡＰを暗号化するようにしているが、非対称暗号で退避対象ＡＰを暗号化するようにしてもよい。この場合には、ＩＣカード２０１は、ステップ１０３では、非対称暗号のアルゴリズムに応じた暗号化鍵を生成するようにする。

【００６９】また、図１に示した動作において、ＩＣカード２０１および端末装置２２１は、ステップ１００およびステップ１１０の相互認証の過程で、一時鍵を共有することができるので、退避ＡＰデータレコード６００を、この一時鍵を用いて暗号通信するようにしてもよい。

【００７０】また、図１に示した動作において、端末装置２２１は、ユーザに退避場所を指定させるようにし、ユーザがキーボード２２４から指定した場所に、退避ＡＰデータレコード６００を格納するようにしてもよい。

【００７１】また、図１に示した動作においては、セキュリティ性をより高めるために、署名による認証技術を利用して、退避ＡＰデータレコード６００がＩＣカード２０１から送信されたものであること、および、退避ＡＰデータレコード６００が改ざんされていないことを確認するようにしているが、これによって本発明の主旨が限定されることはない。

【００７２】次に、本実施形態に係るＩＣカードシステムにおいて、図１に示した動作で退避させたＡＰを回復させる際の動作について、図１０を用いて説明する。

【００７３】図１０は、本実施形態に係るＩＣカードシステムにおけるＡＰ回復時の動作の流れを示す図である。

【００７４】端末装置２２１でＡＰ回復プログラム４０４が起動され、ＩＣカード２０１がＩＣカードリーダ／ライタ２１１に挿入されると、ＩＣカード２０１でＡＰ回復プログラム３０４が起動され、以下の処理が実行される。なお、以下の処理は、ＩＣカード２０１のＭＰＵ２０３および端末装置２２１のＭＰＵ２２３が、ＡＰ回復プログラム３０４およびＡＰ回復プログラムを実行することで実現される。

【００７５】まず、ＩＣカード２０１および端末装置２１１は、図１で説明した動作と同様に、相互認証を行い（ステップ１００，ステップ１１０）、本人認証を行う（ステップ１０１，ステップ１１１）。

【００７６】そして、正しいユーザであることが認証された場合は、ＩＣカード２０１および端末装置２１１は、回復対象ＡＰの指定を行う（ステップ１００２，ステップ１０１２）。

【００７７】回復対象ＡＰの指定においては、詳しくは、まず、端末装置２２１が、ＩＣカード２０１に格納されているＡＰのうちの、退避中のＡＰの一覧を、ＩＣカード２０１から取得してディスプレイ２２５に表示し、ユーザがキーボード２２４から指定したＡＰを、回復対象ＡＰとして、ＩＣカード２０１に通知する（ステップ１０１２）。なお、回復対象ＡＰの通知は、退避対象ＡＰの通知と同様に、ＡＰ指定データレコード５００を送信することで行われる。

【００７８】そして、ＩＣカード２０１が、端末装置２１１からＡＰ指定データレコード５００を受信することで、回復対象ＡＰの指定を受け付ける（ステップ１００２）。

【００７９】続いて、ＩＣカード２０１は、ＡＰ指定データレコード５００を受信すると、回復対象ＡＰのＡＰ管理データリスト７００、および、該ＡＰ管理データリスト７００中のポインタ７０５が示す退避データレコード８００を取り出す（ステップ１００３）。

【００８０】続いて、ＩＣカード２０１および端末装置２１１は、回復対象ＡＰの送受信を行う（ステップ１００４，ステップ１０１３）。

【００８１】回復対象ＡＰの送受信においては、詳しくは、まず、端末装置２１１が、メモリ２２２またはディスク装置等に格納しておいた退避ＡＰデータレコード６００を、回復対象ＡＰとして、端末装置２２１に送信する（ステップ１０１３）。そして、ＩＣカード２０１が、端末装置２１１から退避ＡＰデータを受信することで、回復対象ＡＰを受信する（ステップ１００４）。

【００８２】さて、ＩＣカード２０１は、退避ＡＰデータレコード６００を受信すると、退避ＡＰデータレコード６００中の署名６０４と、ステップ１００３で取り出した退避データレコード８００中の署名８０４とが一致するか否かを確認する（ステップ１００５）。

【００８３】そして、ＩＣカード２０１は、両者が一致することを確認すると、対称暗号系暗号化／復号プログラム３０７を起動することによって、受信した退避ＡＰデータレコード６００中の暗号化ＡＰ６０２を、ステッ

ブ１００３で取り出した退避データレコード８００中の暗号化鍵８０３を用いて復号し、復号した回復対象ＡＰを、ステップ１００３で取り出したＡＰ管理データリスト７００中のファイル情報７０２に従って、メモリ２０２内に再配置する（ステップ１００６）。

【００８４】さらに、ＩＣカード２０１は、回復対象ＡＰのＡＰ管理データリスト７００を更新する（ステップ１００７）。

【００８５】ステップ１００７では、具体的には、ＩＣカード２０１は、ステップ１００３で取り出した退避データレコード８００を消去し、回復対象ＡＰのＡＰ管理データリスト７００中のポインタ７０５に「ＮＵＬＬ」を設定する。

【００８６】以上に説明した動作によって、端末装置２２１に退避させておいたＡＰを、ＩＣカード２０１に回復させることができる。

【００８７】以上説明したように、本実施形態に係るＩＣカードシステムによれば、ＩＣカード２０１に格納されているＡＰを、ユーザの判断で、ＩＣカード２０１から端末装置２２１に退避させることが可能になる。そして、退避対象ＡＰを、ＩＣカード２０１内で生成した暗号化鍵を用いて暗号化するようにしているので、ＩＣカード２０１から退避させられたＡＰは、これを暗号化したＩＣカード２０１以外では復号できず、不正使用されることがない。

【００８８】そこで、特に、ＩＣカード２０１が、ＭＵＬＴＯＳをカードＯＳとしている場合でも、図１に示した動作を行うことで、ユーザの判断で、一時的にＡＰを退避させるようなフレキシブルな運用を実現することができる。

【００８９】ところで、本実施形態に係るＩＣカードシステムにおいては、ＩＣカード２０１に格納されているＡＰを、端末装置２２１に退避させるようにしているが、ＩＣカード２０１のメモリ２０２に余裕がある場合など、暗号化したＡＰをＩＣカード２０１から退避させる必要がない場合には、ＡＰを退避させる代わりに、ＩＣカード２０１内でＡＰを一時的に無効化するようにすることができる。

【００９０】以下、このようにした場合の動作について、図１１を用いて説明する。

【００９１】図１１は、本実施形態に係るＩＣカードシステムにおけるＡＰ無効化時の動作の流れを示す図である。

【００９２】図１１に示す動作は、図１に示した動作と同様であるが、ステップ１１０６において、ＩＣカード２０１が、暗号化したＡＰを、ＩＣカード２０１内に格納するようにした点が異なる。そこで、上述した各種データにおいて、退避／回復させるために必要であった部分には、何も設定されないこととなる。

【００９３】図１１に示した動作によれば、ＡＰを実際には退避させていないが、ＩＣカード２０１内でＡＰを暗号化しているので、第三者の脅威から護ることができる。

【００９４】なお、無効化されたＡＰを有効化する際の動作は、ＩＣカード２０１が、暗号化されて無効化されているＡＰを、これを暗号化したときに用いた暗号化鍵を用いて復号すればよい。

【００９５】また、図１１に示した動作を行うようにする場合には、端末装置２２１において、ＡＰを退避させるか、または、無効化させるかという選択を、ユーザに指定させるようにする必要がある。

【００９６】また、図１１に示した動作は、図１に示した動作とは独立に行うことが可能である。すなわち、図１１に示した動作のみを行うＩＣカードシステムを構築することが可能である。

【００９７】なお、以上の説明では、退避対象および無効化対象とするデータがＡＰであるものとしているが、ＡＰ以外の他のデータであってもよいことは、説明するまでもない。

【００９８】

【発明の効果】以上説明したように、本発明によれば、ＩＣカードに格納されているデータを、ユーザの判断で、ＩＣカードから退避させることが可能になる。そして、退避させるＡＰを、ＩＣカード内で生成した暗号化鍵を用いて暗号化するようにしているので、ＩＣカードから退避させられたデータは、これを暗号化したＩＣカード以外では復号できず、不正使用されることがない。

【図面の簡単な説明】

【図１】本実施形態に係るＩＣカードシステムにおけるＡＰ退避時の動作の流れを示す説明図。

【図２】本発明の実施形態に係るＩＣカードシステムの全体構成図。

【図３】本発明の実施形態におけるＩＣカードのメモリに格納されている内容を示す説明図。

【図４】本発明の実施形態における端末装置のメモリに格納されている内容を示す説明図。

【図５】本発明の実施形態におけるＡＰ指定データの一例を示す説明図。

【図６】本発明の実施形態における退避ＡＰデータの一例を示す説明図。

【図７】本発明の実施形態におけるＡＰ管理情報の一例を示す説明図。

【図８】本発明の実施形態における退避データの一例を示す説明図。

【図９】本発明の実施形態における署名生成用データの一例を示す説明図。

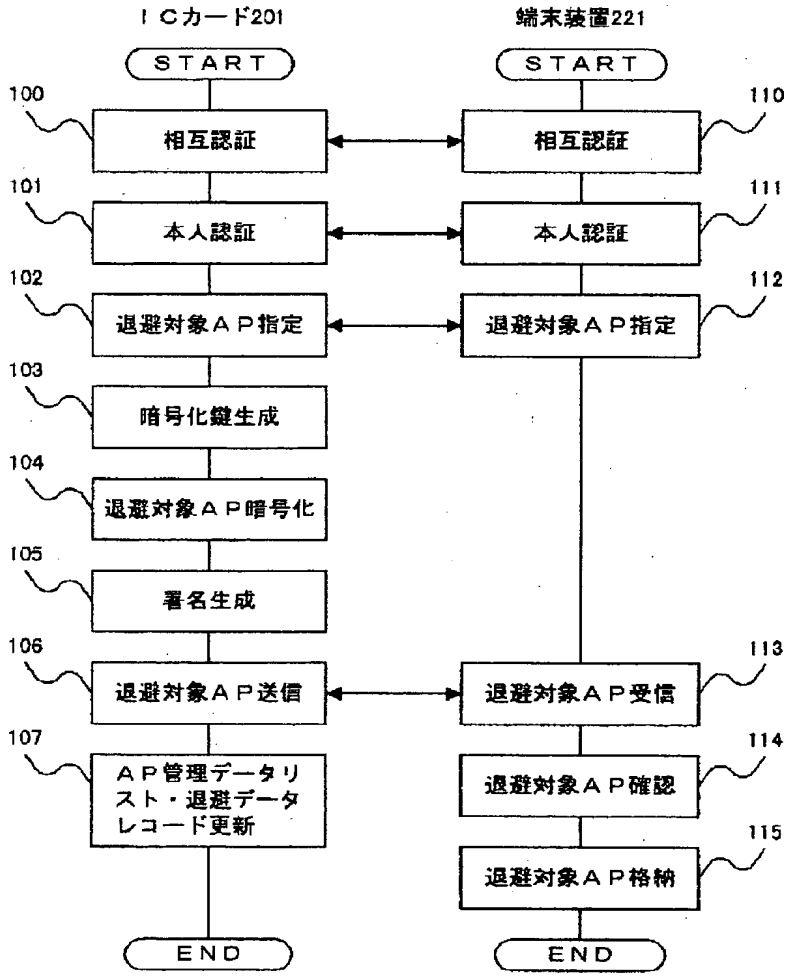
【図１０】本実施形態に係るＩＣカードシステムにおけるＡＰ回復時の動作の流れを示す説明図。

【図１１】本実施形態に係るＩＣカードシステムにおけるＡＰ無効化時の動作の流れを示す説明図。

【符号の説明】
２０１…ＩＣカード、２１１…ＩＣカードリーダ／ライタ、２２１…端末装置、２０２，２２２…メモリ、２０３，２２３…ＭＰＵ、２０４，２１２，２１３…送受信ＩＦ、２２４…キーボード、２２５…ディスプレイ、５＊＊００…ＡＰ指定データレコード、６００…退避ＡＰデータレコード、７００…ＡＰ管理データリスト、８００…退避データレコード、９００…署名生成用データレコード。

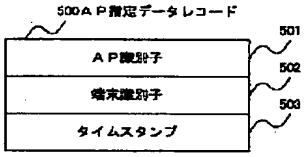
【図１】

図 1



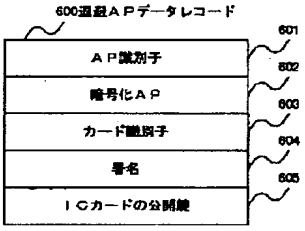
【図５】

図 5



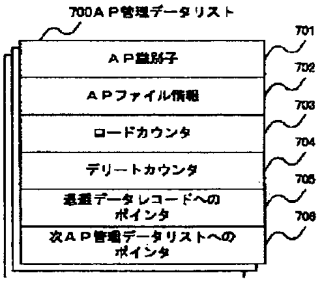
【図６】

図 6



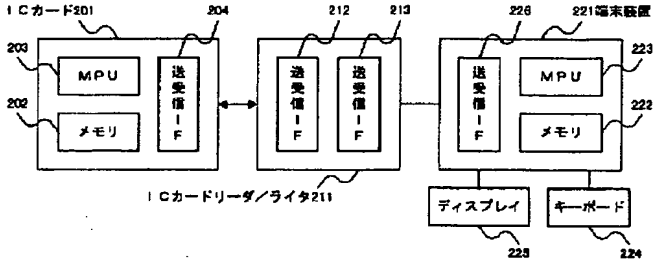
【図７】

図 7



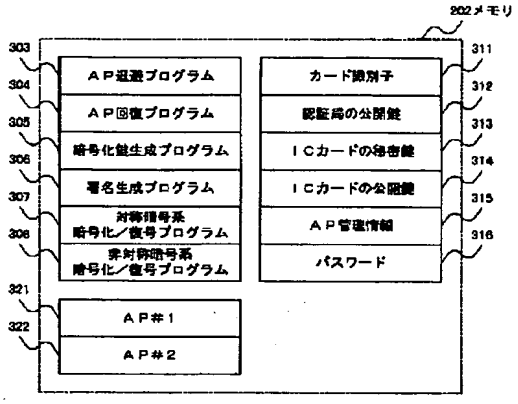
【図２】

図 2



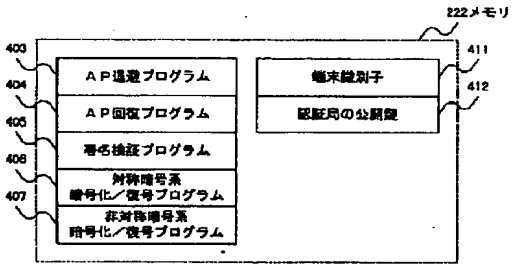
【図３】

図 3



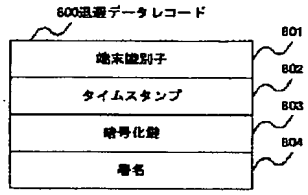
【図４】

図 4



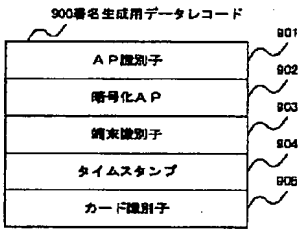
【図８】

図 8



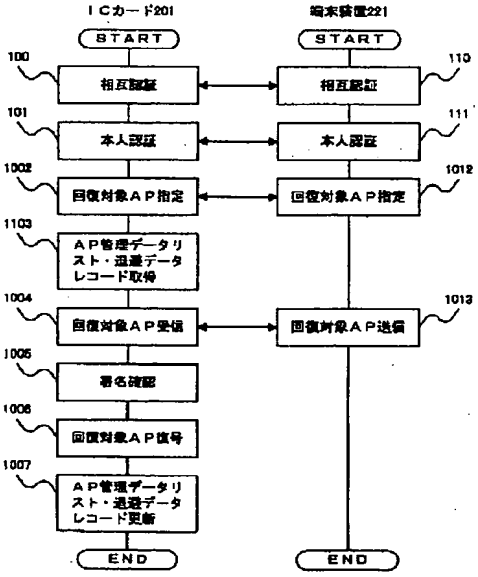
【図９】

図 9



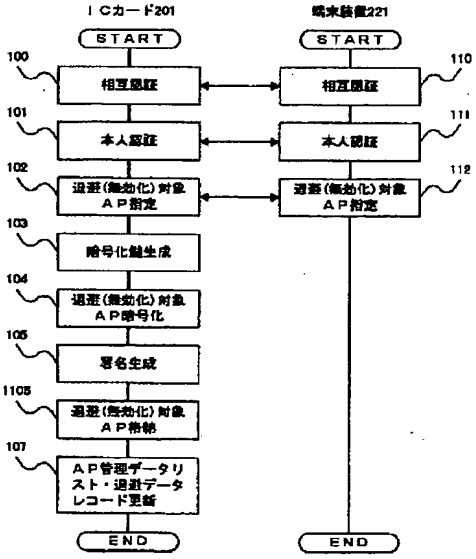
【図１０】

図 10



【図１１】

図 11



フロントページの続き

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	N

(72)発明者　原口　政敏
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

Ｆターム(参考)　5B035 AA13 BB09 BC03 CA29 CA38
5B058 CA27 KA01 KA04 KA35 YA13
5B065 BA09 PA16